网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

乱雲飛渡

资源代价与安全算力

云环境威胁猎杀实践与思考

安天 | 安全服务中心

CONTENTS

目 录

01 云上威胁猎杀方法

上云后的安全威胁

云上安全事件频发

Gartner副总裁兼云安全负责人Jay Heise：“云中的安全不仅在于云服务提供商，还在于云客户”。

事件时间	事件内容	事件涉事方	事件后果
2020.1.19	Cloudflare泄露用户HTTPS网络会话中的加密数据	Cloudflare	预计至少200万家网站受影响，其中涉及Uber等多家知名互联网公司
2020.1.21	土耳其“图兰军”对我国网站发起攻击	中国站点	影响网络正常秩序
2020.2.23	微盟运维人员删库	微盟	微盟市值一天之内蒸发超10亿元，数百万用户受到直接影响
2020.3.16	微软Teams平台涌入大量新用户导致宕机	微软	导致该服务在欧洲地区出现持续2小时的宕机
2020.3.26	谷歌云再次宕机	谷歌	Google多个云服务无法访问
2020.4.10	华为云大面积宕机	华为	华为云登录、管理后台无法访问，本次宕机持续约三小时
2020.4.8	Google Cloud身份和访问管理出现故障	谷歌	导致多个Google服务中断，包括App Engine及其核心Compute Engine IaaS
2020.5.28	Adobe Creative Cloud发生宕机	Adobe	故障波及包括Photoshop、InDesign等备受欢迎的产品
2020.6.2	苹果iCloud云存储服务宕机	苹果	导致一些用户无法顺利登录iCloud账户，无法访问Web应用程序
2020.6.9	IBM云计算发生长达四个小时的中断故障	IBM Cloud	导致多项托管于平台上的互联网服务中断，其中包括知名聚合网站Techmeme
2020.7.8	上海孝信网络数据泄露	孝信网络	超过34万条的GPS位置信息、手机号、地址等敏感信息记录被泄露
2020.8.10	Muhstik僵尸网络大肆攻击国内云服务器	国内多家知名企业	已有数千台服务器失陷
2020.10.7	Microsoft Office 365办公软件和Azure云产品出现故障	微软	导致部分用户服务中断数小时
2020.11.25	亚马逊云服务出现中断，本次宕机持续约5小时	亚马逊	大量网站和服务受到影响
2020.12.14	谷歌云宕机	谷歌	包括YouTube、Gmail在内的多个Google云服务遭受约一个小时大面积宕机
2020.12.22	蔓灵花组织利用病毒邮件对我国关键领域发动钓鱼邮件攻击	部分政府部门	窃取机密文件
2020.12.30	T-Mobile用户数据泄露	T-Mobile	手机号和通话记录泄露，影响的人数约20万
2021.1.26	TikTok漏洞引发数据和隐私泄露	TikTok	引发数据和隐私泄露
2021.2.21	钓鱼邮件攻击	红杉资本	投资者的个人信息和财务信息已被第三方窃取
2021.3.21	某电脑制造商北美地区据点遭到名为REvil的勒索病毒攻击	某电脑制造商	黑客勒索5,000万美金的赎金，折合人民币约3.26亿元

2020.1 ~ 2021.3 20起重大云安全事件

云计算的11大威胁

1. 数据泄露
2. 配置错误和变更控制不足
3. 缺乏云安全架构和策略
4. 身份、凭证、访问和密钥管理不善
5. 账户劫持
6. 内部威胁
7. 不安全的接口和API
8. 控制面薄弱
9. 元结构和应用程序结构故障
10. 云资源使用的可见性差
11. 滥用和恶意使用云服务

勒索软件威胁

- 勒索软件在依然保持活跃
- 攻击目标从“遍地撒网”演变成了“重点捞鱼”
- **越来越多的定向攻击出现，特别是针对企事业单位**

恶意挖矿威胁

- 数字货币价格一路飙升，挖矿事件层出不穷。
- 虽然数字货币浪潮不断退去，**但目前仍是应急响应事件中数量最多的类型之一。**

云安全责任共担要求

依据《**信息安全技术 网络安全等级保护基本要求 第2部分：云计算安全扩展要求**》，就云服务商与云租户的责任分担进行了更为细致的梳理基于不同云计算服务模式，需要采取不同职责划分方式：

IaaS基础设施服务模式

云服务商　虚拟机监视器 、硬件

云租户　操作系统、中间件 、应用数据。

PaaS平台即服务的服务模式

云服务商　硬件、虚拟机监视器、操作系统和中间件

云租户　应用和数据。

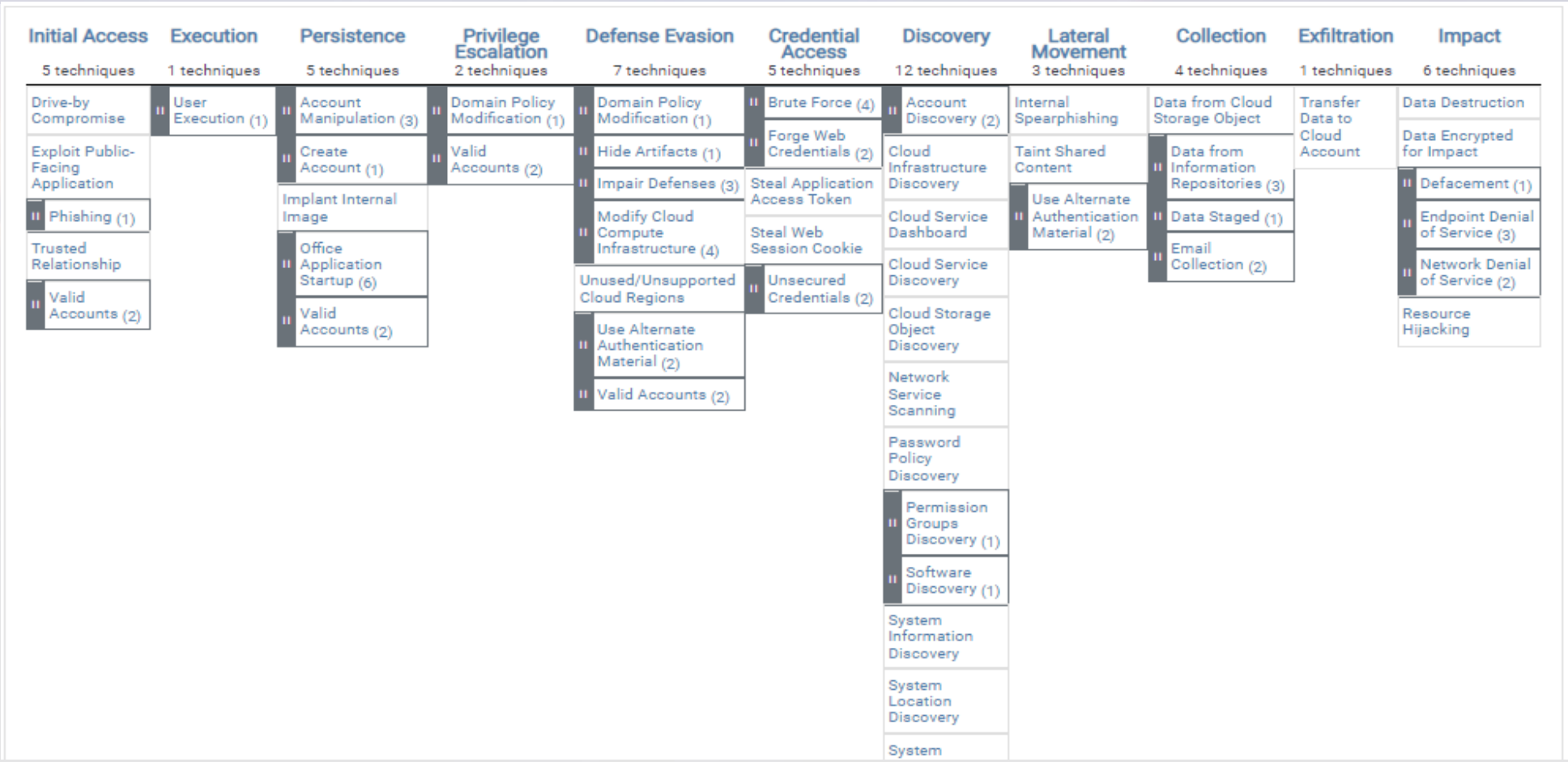
SaaS软件服务模式

云服务商　硬件、虚拟机监视器、操作系统、中间件和应用

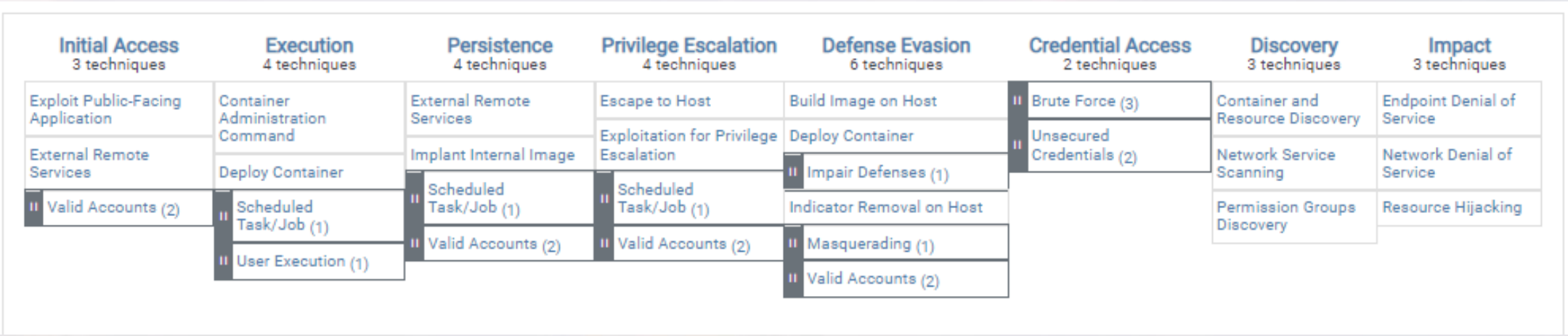
云租户　应用及用户使用

	安全要求	IaaS	PaaS	SaaS
技术要求	应用和数据安全	双方共担	双方共担	双方共担
	设备和计算安全	双方共担	云服务商	云服务商
	网络和通信安全	双方共担	云服务商	云服务商
	物理和环境安全	云服务商	云服务商	云服务商
管理要求	系统安全运维管理	双方共担	云服务商	云服务商
	系统安全建设管理	双方共担	双方共担	双方共担
	安全管理机构和人员	云服务商	云服务商	云服务商

从MITRE ATT&CK 视角看云主机网络攻击



从MITRE ATT&CK 视角看容器安全网络攻击



云上威胁猎杀概念

威胁猎杀是**深入的、以“人”为主导**的**调查过程**，旨在发现关键信息资产中**潜伏的威胁。**是**积极防御层面**一种**主动和迭代**的**威胁检测方法**，其目的是在**攻击者对关键信息资产造成任何损害之前阻止它们。**





猎：发现、关联/拓线、寻踪

杀：排查、处置、加固

威胁猎杀的支撑三要素

猎手依赖自动化工具
工具的有效性取决猎手水平

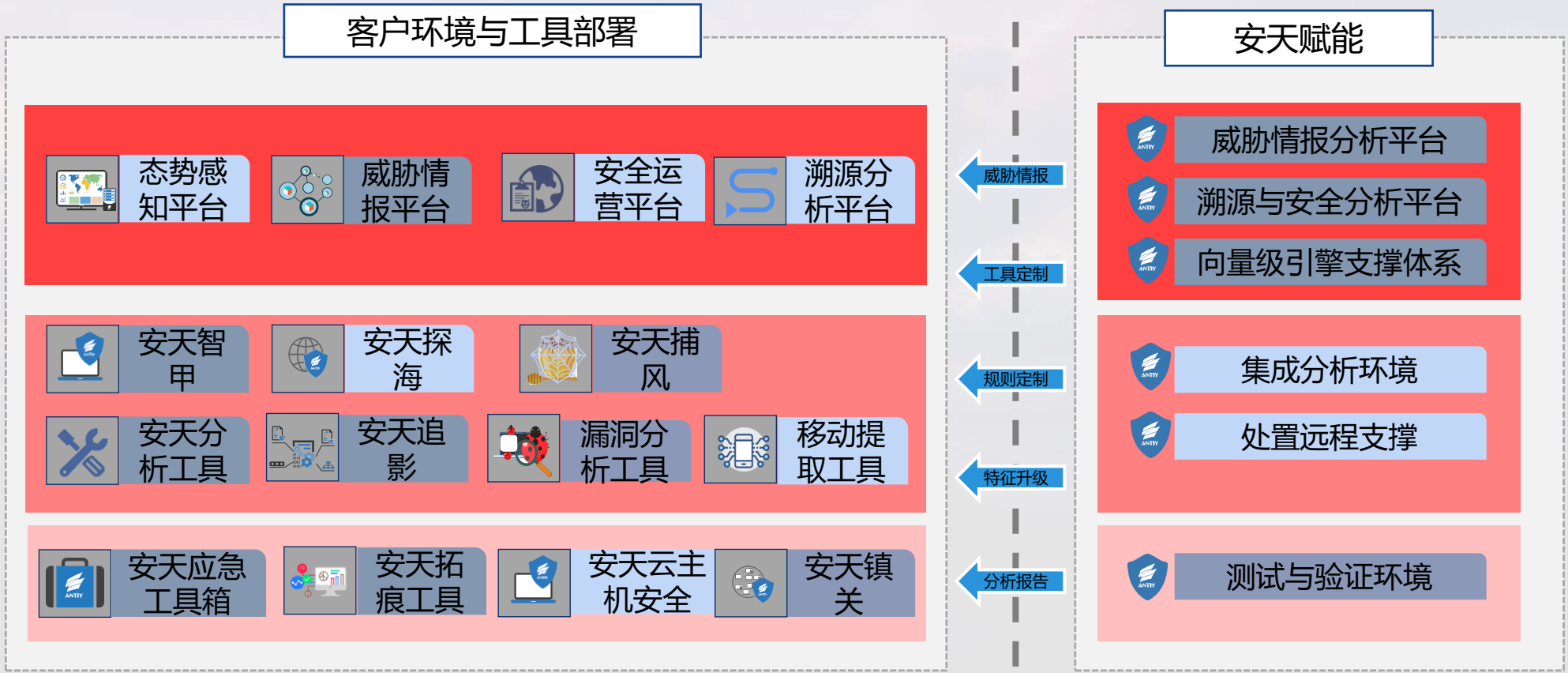
猎手分析数据生产知识
数据与知识为猎手提供线索

工具进行数据采集和处理、辅助情报与知识生产

威胁猎杀的支撑要素-人员团队

	角色名称	角色职责	能力要求
	威胁猎杀分析师	负者对监控的到全流量和日志信息进行分析，找出异常和可疑信息，并进行分析，提出/更新假设，给出需要取证的清单列表；	网络协议分析技术、异常分析、日志分析、大数据分析、关联分析等等
	现场工程师	负者对取证清单列表进行取证； 负者对处置指南进行处置； 负者对来自外部情报和内部情报进行收集整，将情报中的IOC、TTP等	网络协议分析技术、全平台取证技术、数据库取证、数据恢复技术、对应工具使用等
	逆向分析工程师	负者对恶意样本的解剖分析，对样本的网络特征和文件特征进行提取，提取后的特征会分发给各产品下发规则进行排查，形成排查工具等，最后分析师通过关联分析和朔源分析形成分析报告。	高级威胁分析、二进制深度逆向分析、取证分析、工具开发等、
	指挥协调员	负者指挥排查处置工作和与客户侧人员协调等工作；	全局视野和全面的知识体系、沟通能力、表达能力等
	客户系统管理员	负责设备安装调试工作 ； 负责协助取证工作、部署/增补信息采集点； 负责协助现场工程师进行排查处置工作；	网络规划、日常运维、网络结构、网络设备安装调试、网络协议、故障检测等
	客户控制工程师	负责协助在工控系统中的取证工作、部署/增补信息采集点； 负责协助现场工程师进行排查处置工作；	掌握工控系统结构、工控协议、工控软件和仪表操作等
	客户安全管理员	负责协助取证工作、部署/增补信息采集点； 负责协助现场工程师进行排查处置工作；	网络安全设备使用、安全知识等
	厂商维护工程师	负责协助现场工程师进行排查处置工作；	对自身出品的各种软硬件系统进行安装、调试、维护的能力。

威胁猎杀的支撑要素-工具



威胁猎杀的支撑要素-数据与知识

多源情报数据

- HASH
- IP/域名/URL/DNS
- 组织信息
- 攻击者信息
- 样本向量信息
- ……

安全运行数据

- 防火墙日志和配置信息
- IPS、IDS日志和配置信息
- 边界日志数据
- VPN日志和配置信息
- ……

知识与增补数据

- 探海(NDR)采集流量
- 智甲(EDR)采集主机要素
- 追影动态分析完善行为数据
- 威胁对抗知识
- 取证/分析报告
- …

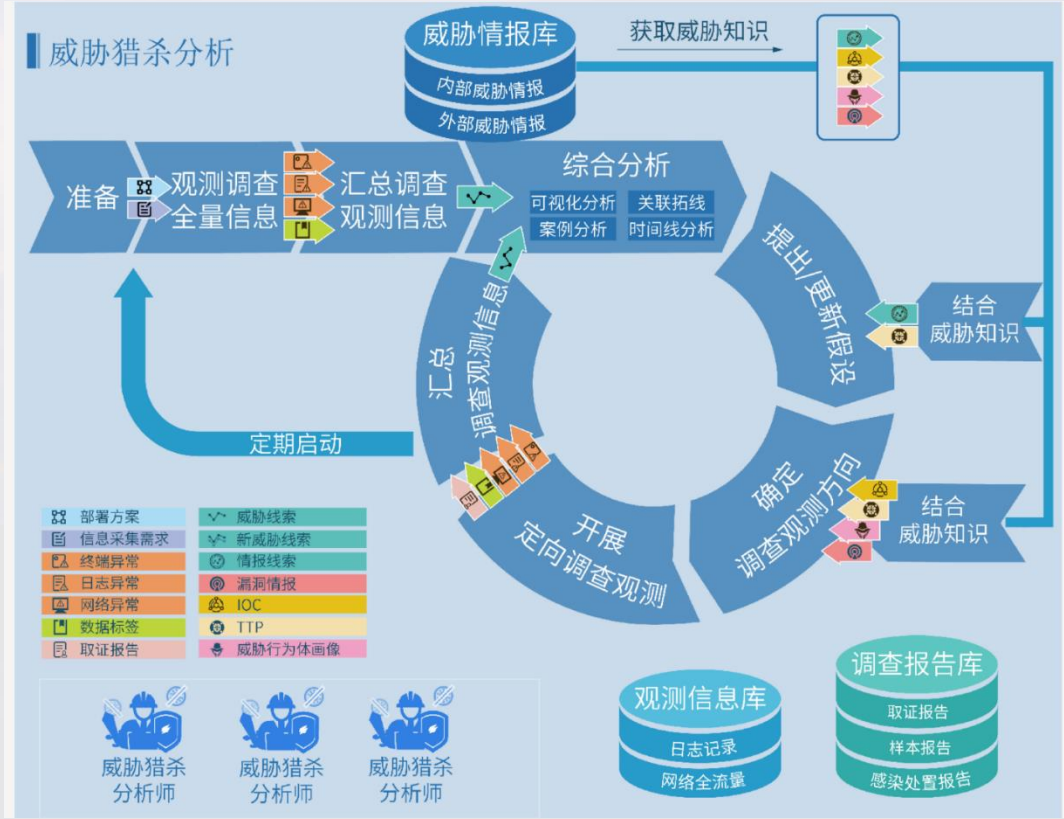
基础数据

账户信息、软件硬件资产信息、 IP通联和网络拓扑等

威胁猎杀的三个工作层面

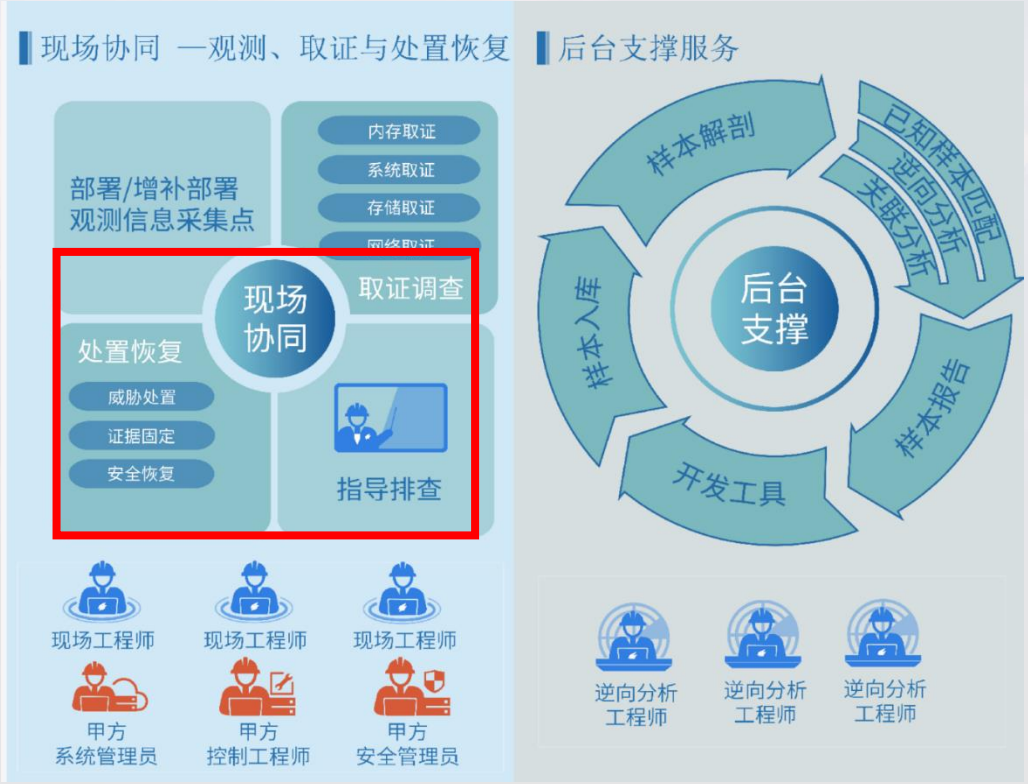
威胁猎杀分析

- 信息系统需具备全量信息采集能力
  - 如果没有可以临时部署探海
  - 终端亦可通过工具手工采集
- 全量观测、排查已知、分析异常
  - 不符合业务场景的“白流量”
  - P2P等隐蔽通讯的网络流量
  - 不常用的端口、字符、扩展名
  - 格式与扩展名不一致
  - 非系统目录下的系统程序
  - 快捷方式中调用系统命令或脚本
- 汇总调查、形成线索
- 综合分析
  - 可视化分析
  - 关联拓线分析
  - 案例分析
  - 时间线分析
- 提出假设、用事实验证或排除



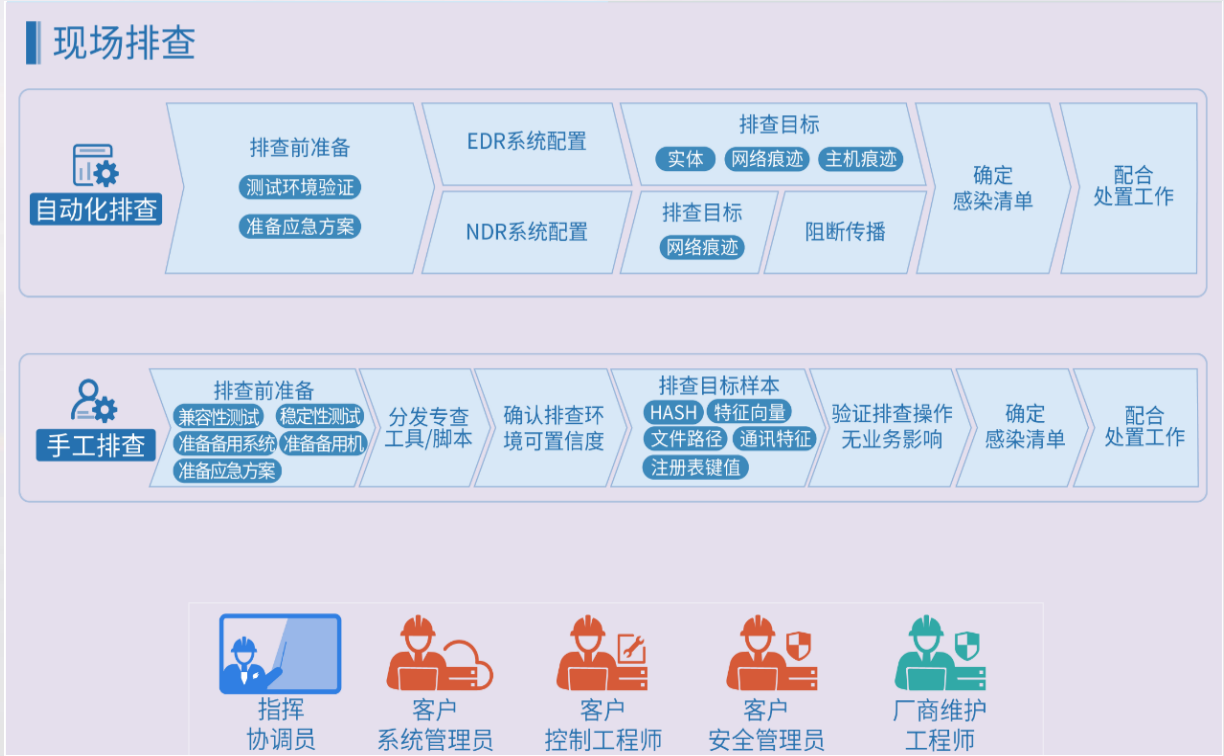
现场协同与后台支撑

- 观测、取证与处置恢复需要现场协同
  - 现场工程师
  - 客户系统管理员
  - 客户控制工程师
  - 客户安全管理员
- 对于所需分析开发工作需要后台支撑
  - 逆向分析工程师
  - 威胁猎杀工程师



现场排查

- 现场排查
  - 自动化排查，对于包含EDR/NDR等安全防御措施的业务系统场景，基于特征包及其加载指南进行自动化排查；
  - 手工排查，对于无法进行自动化排查的业务系统场景，则基于专查工具及其使用手册开展手工排查。



威胁猎杀的核心——提出和更新假设

假设是建立在观察之上有根据的猜测，是潜在的解释或结论，需要通过搜集和提出证据来进行检验，好的假设能够带来好的猎杀。

可被验证和证伪

即至少在可以访问的数据中能够找到它们的蛛丝马迹

以异常和威胁知识为基础

威胁分析师可以基于观察到的异常结合威胁知识形成对环境中持续威胁活动的猜想，提出相应的假设。

是确切的称述，而非问题

威胁猎杀分析师在观察的过程中，会产生很多的想法。在生成假设的时，如果无准确的表达某个想法，或者发现它太含糊，那么它就不是一个好的想法。

包括一个因变量和一个自变量

即一个“何事”与一个“为何”；
因变量是被解释的现象，自变量做出了解释。

从“敌情不明”到“洞悉敌情”的迭代循环

02 威胁猎杀实践案例

案例1 - 背景与需求

- 2021年5月，安天受某大型互联网公司邀请，在云环境中对其云主机及云上运行的信息系统开展威胁猎杀服务。意在检测云环境中是否存在APT样本及攻击痕迹，实现早发现、早预防、及时整改网络安全风险。
- 本次排查范围包括500余台云主机及运行的信息系统，网络架构复杂、日志较多。在此背景下，用户要求1-2周内完成威胁猎杀工作。
- 本次排查前，安天公司与该用户有引擎授权合作，该用户自研的EDR采用了安天AVL引擎，部分云主机已安装其自研EDR，为完成本次威胁猎杀任务，还需全面补充监测、分析、处置能力。

案例1 - 实施

- 主要工具：智甲云主机安全系统

资产清点

对主机的软硬件资产进行管理，并对账号、进程、软件、Web业务、数据库等资产进行详细的清点。

合规基线

CIS基线、等保2.0基线

微隔离

以应用为中心进行访问控制和网络拓扑展示，使应用间的风险可视，相关的网络连接清晰可见。

威胁情报

通过云端提供威胁情报服务，提升威胁检测等的能力。

风险发现

通过补丁检测、漏洞扫描、安全监测、弱口令检测等手段主动发现系统的安全风险。

威胁检测

实时检测入侵事件，提供告警和保护能力。

容器安全

针对容器生命周期进行安全防护，提供强大的实时监控和响应能力，保障企业的容器环境安全。

蜜罐

支持虚拟机和容器形式的蜜罐，支持对蜜罐的编排调度。

案例1 - 实施

- 主要工具：威胁情报分析系统

- 支持域名当前解析记录和历史解析记录。
- 支持域名WHOIS记录和历史解析记录。
- 数据量超过20亿，每日更新10万。

- 支持md5、sha1、sha256查询文件信誉。
- 支持输出静态/动态执行信息、多引擎扫描结果。
- 数据量超过30亿，每日新增百万。

- 涵盖操作系统的常见注册表键值。
- 支持输出使用注册表的样本。
- 规则数量超过万条。

- 收集APT报告数量超过700份
- 跟踪组织或行动超过180个，涉及14个国家和三个地区

- 涵盖CVE、CNNVD编号查询。
- 支持资产(CPE)搜索受影响的漏洞。
- 漏洞数据量超过10万个，每天更新

- 支持查询地理位置、ASN归属、开放端口、服务、应用等信息。
- 支持当前IP反向解析域名和历史解析记录。
- 数据量涵盖全部IPv4,每日更新十万。

- 支持输出URL关联的通讯样本，从URL下载样本、样本静态分析出的URL
- 数据量超过10亿，每日更新10万

案例1 - 实施

01 建立覆盖全网的终端监测、分析、处置能力

02 智甲结合多引擎对照分析系统，完成威胁初筛

03 智甲结合威胁情报分析系统，完成威胁拓线与关联分析

04 威胁处置、观察跟进、持续监测

案例1 - 实施

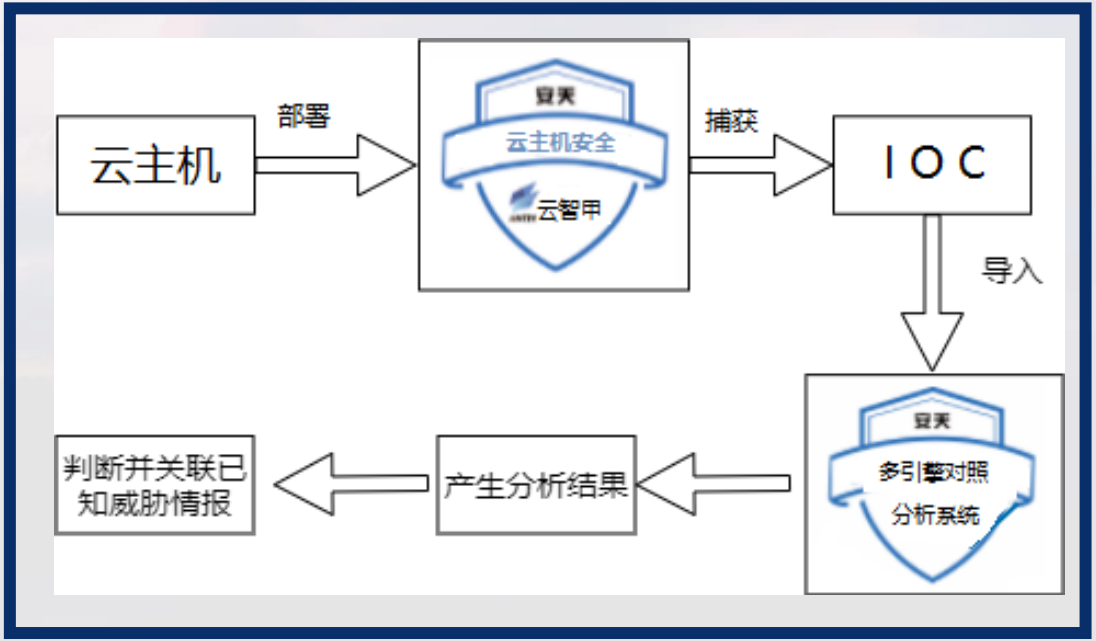
- 威胁检测：智甲云主机安全+多引擎对照分析系统

a. 在用户所有云主机中部署**安天智甲云主机安全防护系统**。

b. 智甲将在云主机中捕获的到样本、MD5、回连域名等**IOC**导入安天**多引擎对照分析系统**中。

c. 多引擎对照分析系统对导入的IOC实施对照分析，得出综合对照分析结果。

d. 分析人员根据上述结果**人工验证**。



案例1 - 实施

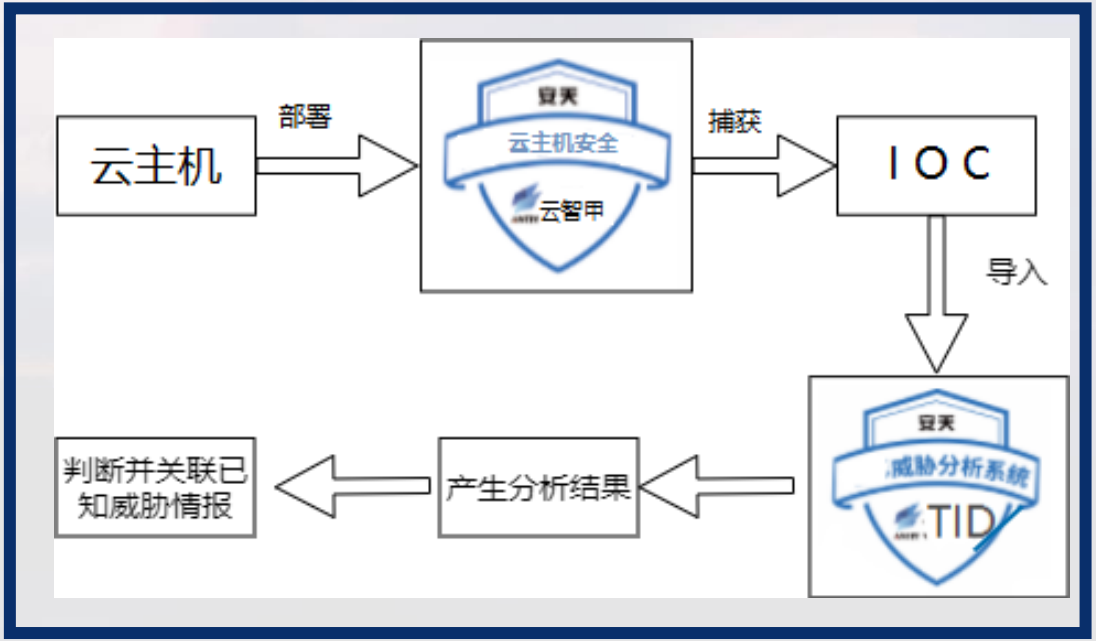
- 威胁检测：智甲云主机安全+威胁情报分析系统

a. 在用户所有云主机中部署**安天智甲云主机安全防护系统**。

b. 智甲将在云主机中捕获的到样本、MD5、回连域名等**IOC**导入安天**威胁情报分析系统**（TID）中。

c. TID对导入的IOC实施威胁**拓线**与**关联分析**产生分析结果。排查是否存在与APT相关的IOC。

d. 分析人员结合**多引擎对照分析**的结果与**TID**关联分析的结果实施**分析研判**。



案例1 - 实施

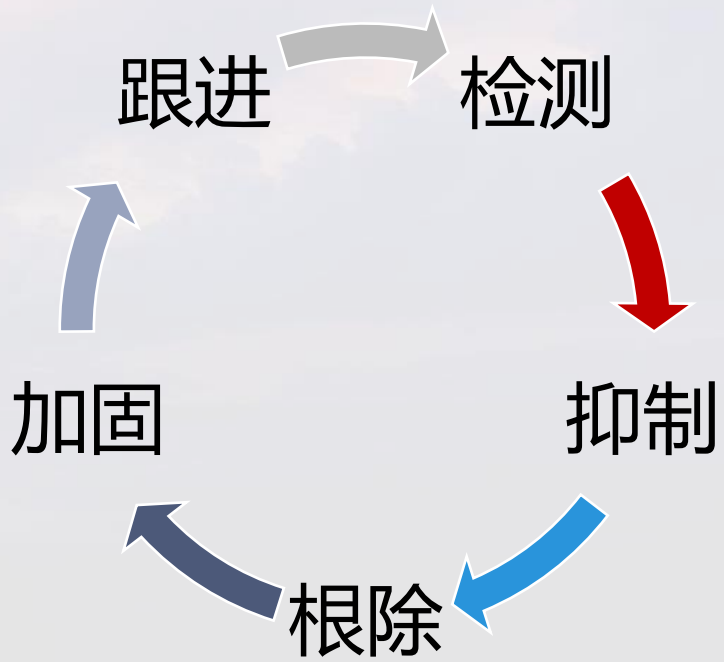
- 威胁处置：

a. 利用安天应急响应工具箱（EHT），结合威胁狩猎阶段的结果，对受害机实施取证分析。

b. 利用用户边界防护设备配置相关阻断策略，防止发生二次攻击。

c. 利用智甲云主机安全防护产品实施威胁处置，包括恶意代码清除与安全加固。

d. 完成威胁处置后，持续监测72小时，确保所有威胁已完成清除。恢复系统化至正常运行状态。



案例1 - 总结

- 企业用户的云上安全运营目前尚处于起步阶段，面临APT组织日渐成熟的攻击手法与层出不穷的安全隐患，企业用户的云资产已成为众多APT组织的首要攻击目标。
- 当云上环境无法使用传统流量监测的方式实施威胁监测时，利用云主机侧的探针类产品也能起到同类效果。
- 威胁猎杀是一种主动防御手段，并非局限于发生安全事件后的应急响应。需在日常安全运营中定期、持续开展，提升网络安全防御能力。

案例二——背景与需求

- 2021年某日，能源电力行业某集团公司被国际知名勒索组织攻击，被入侵后受到了攻击者的双重勒索（窃取数据进行勒索，不支付赎金就公开数据；传播勒索病毒至上千台主机被加密勒索，不支付赎金就无法解密数据）

- 用户需求包括：溯源整个攻击过程、清除潜伏的威胁、提供有针对性的加固整改方案，避免再次发生类似事件

- 面临的困难：复杂的网络环境（国外多个国家有办事处，国内多个城市有分公司）；网内主机数量庞大，1万余台主机；海量的日志记录信息，并且部分日志被攻击者删除

案例二——受害用户能力VS高级网空威胁行为体能力

- 敌已在内、敌情不明
- 传统安全设备
- 云基础设施基础防护
- 传统威胁基础对抗经验

用户能力

受害用户

安天赋能

- 高水平分析团队
- 高水平威胁对抗团队
- 威胁情报赋能
- NDR、RAS、UES产品赋能

- 团队化作业，分工明确
- 成熟商用军火平台
- 加密流量混淆
- 多重加密shellcode

行为能力

高能力网空威胁行为体

作战实力

- 对主流杀软免杀
- 无实体文件落地
- 关闭UAC、杀软
- 删除主机日志

案例二——溯源分析思路

溯源过程是一个逆向的过程，知道事件表象的结果。通过猎杀工程师搜集证据、人工分析证据找到攻击线索不断向前推导，直至找到攻击源头，最后按照时间顺序和前后逻辑关系还原整个事件攻击过程

信息搜集	• 了解事件的背景，整体的网络结构，互联网和内网资产情况，邮件系统，VPN，网络侧与主机侧安全措施等
提出假设	• 站在攻击者的视角思考，面对当前网络场景中的攻击入口，提出能够达到当前的攻击效果的可用的攻击手段假设，然后通过搜集相关证据进行分析逐个验证或排除。
分析协同	• 前后端协同作战，前端人员现场取证分析，后端专家团队分析恶意代码与威胁情报支撑
还原事件	• 将分析出来的攻击源头，以及各个阶段的攻击线索，按时间顺序与合理的攻击逻辑关系串联起来还原整个事件攻击过程

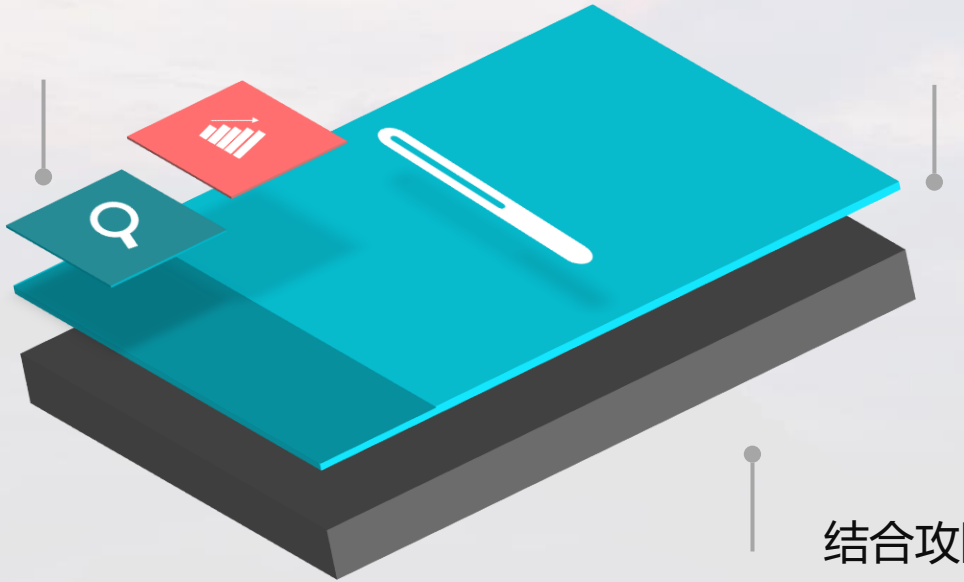
案例二——溯源分析方向

对病毒样本进行分析

1. 掌握恶意代码的网络行为和本地行为
2. 通过安天威胁情报平台关联分析发现与宜家被钓鱼攻击传播的Qbot样本相似

针对云出网流量进行分析

1. 通过安天探海结合威胁情报发现攻击者C2地址
2. 定位受害主机，明确全网猎杀范围



针对日志进行分析

1. 分析系统日志，发现入侵痕迹与横向传播线索
2. 分析防火墙日志，指定时间周期内发现其他主机与受害主机的连接关系，找到更多受侵害的主机

结合攻防作业流程进行分析

站在红队视角，结合当前场景和攻击线索，梳理攻击作业流程

案例二——实施工具

威胁情报平台（TID）

对全球APT组织行动的持续追踪与分析，输出高质量的自有威胁情报库、威胁知识库，结合外部情报，提供快速查询与获取威胁情报能力

探海威胁检测系统（PTD）

安天探海威胁检测系统基于自定义场景化规则，结合威胁猎杀情报，发现C2地址，明确失陷损失。

应急处置工具箱（EHT）

安天拓痕检出和留存攻击载荷，提取可疑对象，并通过底层处置能力，清除钓鱼文件、软件等威胁，完成威胁发现、分析、取证、处置业务闭环。

智甲终端防御系统（IEP）

安天智甲终端防御系统针对端点侧进行勒索阻断、定点清除、追踪溯源

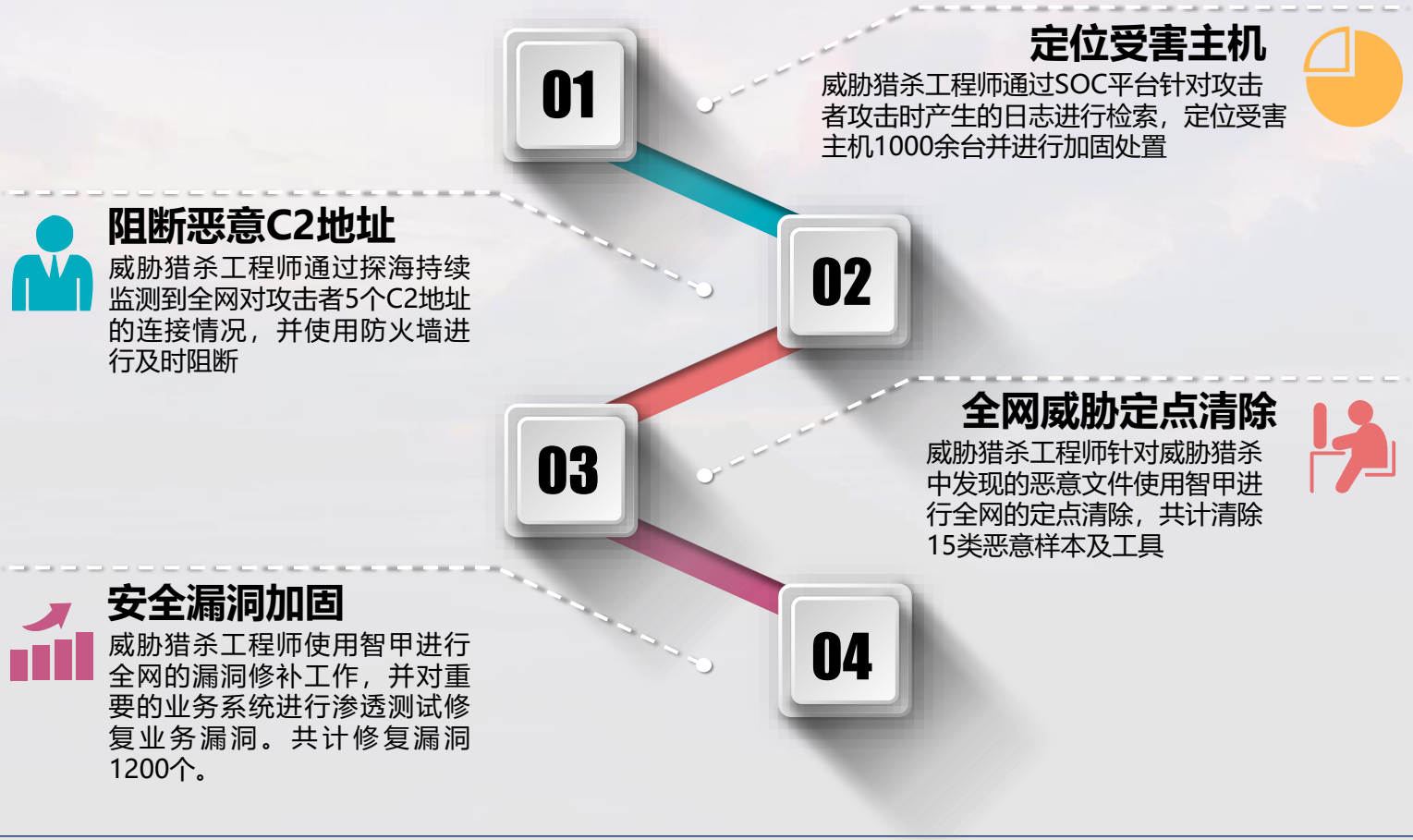
案例二——攻击过程溯源

阶段	时间	行为
初始控制	2021年某日	某国际知名黑客组织入侵了该集团在亚洲A国办事处员工主机（零号主机）
横向渗透	2天后	黑客组织通过零号主机接入欧洲某国VPN 黑客组织使用零号主机通过欧洲某国VPN控制了国内数据中心云DC域控1 黑客组织通过国内DC域控1控制并窃密了亚洲J国云存储服务器 黑客组织通过亚洲J国云存储服务器控制了亚洲T国考勤机（10. *.*.*.*）
窃取数据	3天后	黑客组织通过亚洲J国云存储服务器控制并窃密了业务服务器1（10. *.*.*.*） 黑客组织通过亚洲J国云存储服务器控制了业务服务器2（10. *.*.*.*） 黑客组织通过亚洲J国云存储服务器控制了业务服务器3（10. *.*.*.*） 黑客组织通过亚洲J国云存储服务器控制了业务服务器4、业务服务器5
传播勒索	9天后	黑客组织利用了亚洲T国考勤机（10. *.*.*.*）控制了亚洲J国域控（10. *.*.*.*）作为跳板 黑客组织利用亚洲J国域控（10. *.*.*.*）作为跳板控制了国内某数据中心域控（10. *.*.*.*） 黑客组织利用国内数据中心域控（10*.*.*.*）向1000+台受害主机下达指令传播勒索病毒

案例二——攻击手法还原

攻击路径	手段	分析方法
鱼叉式钓鱼攻击获取员工PC权限	1. 精准钓鱼亚洲A国办事处某工作人员 2. 落地包含远控、信息收集功能的宏病毒文档	排查可疑邮件、PC机被控制情况
横向渗透拿下域控	1. 利用员工PC机作为跳板发现域控，获取内存中的账号密码吗 2. 使用mimikatz工具的ZeroLogon漏洞（CVE-2020–1472）模块对域控进行攻击	1.审计域控日志，尤其是针对ID 58XX类、47XX、46XX,的事件 2.IDS、防火墙上关注端口扫描行为、IP资产遍历行为
窃密回传文件	1. 使用mimikatz、ntds.dit获取域控密码、系统密码 2. 避免不出网场景，使用smb监听器方式 3. 使用powershell作为无实体文件方式进行控制	1. 取证受害主机，解密powershell脚本 2. 排查短时间内大量访问的公网地址，结合威胁情报分析IP地址的
通过域控大范围传播勒索	1.通过CS安装psexec服务，其中需要利用前期抓取的密码 2.利用smb监听器进行监听，释放bat和exe文件进行勒索 3.扫描网内445端口，利用SMBGhost漏洞、ms17-010漏洞获取更大范围权限	网络与主机日志分析、样本深入分析

案例二——全网威胁检测与阻断

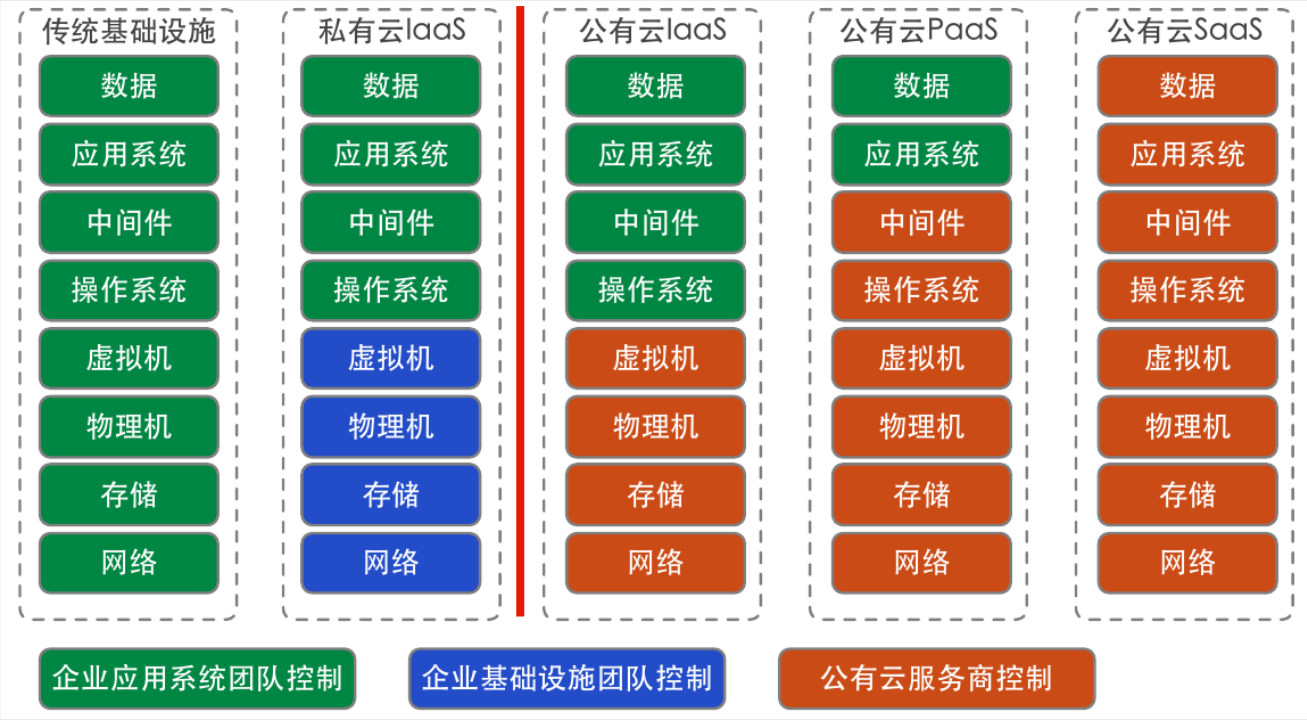


案例二——总结与思考

- 攻击组织为了牟利最大化，攻击方式已经从广撒网式传播变得更有针对性，开始不断寻找高价值目标，然后单点突破、内网横向渗透，窃取高价值数据进行勒索、大规模勒索加密进行勒索等方式迫使受害用户支付赎金；
- 网络军火的滥用大大降低了网络攻击的门槛，其带来的流量加密、无实体文件落地、漏洞模块化的特性极大的提高了威胁对抗的成本；
- 通过云端流量捕获、端点侧威胁发现，结合威胁情报与专业的威胁猎杀团队，可以迅速响应并处置未知威胁；
- 云上系统建设时云租户应遵循“最小化原则”和统一周期补丁管理；网络安全建设应当从高对抗与持续性安全运营的角度进行。

03 云上威胁猎杀思考

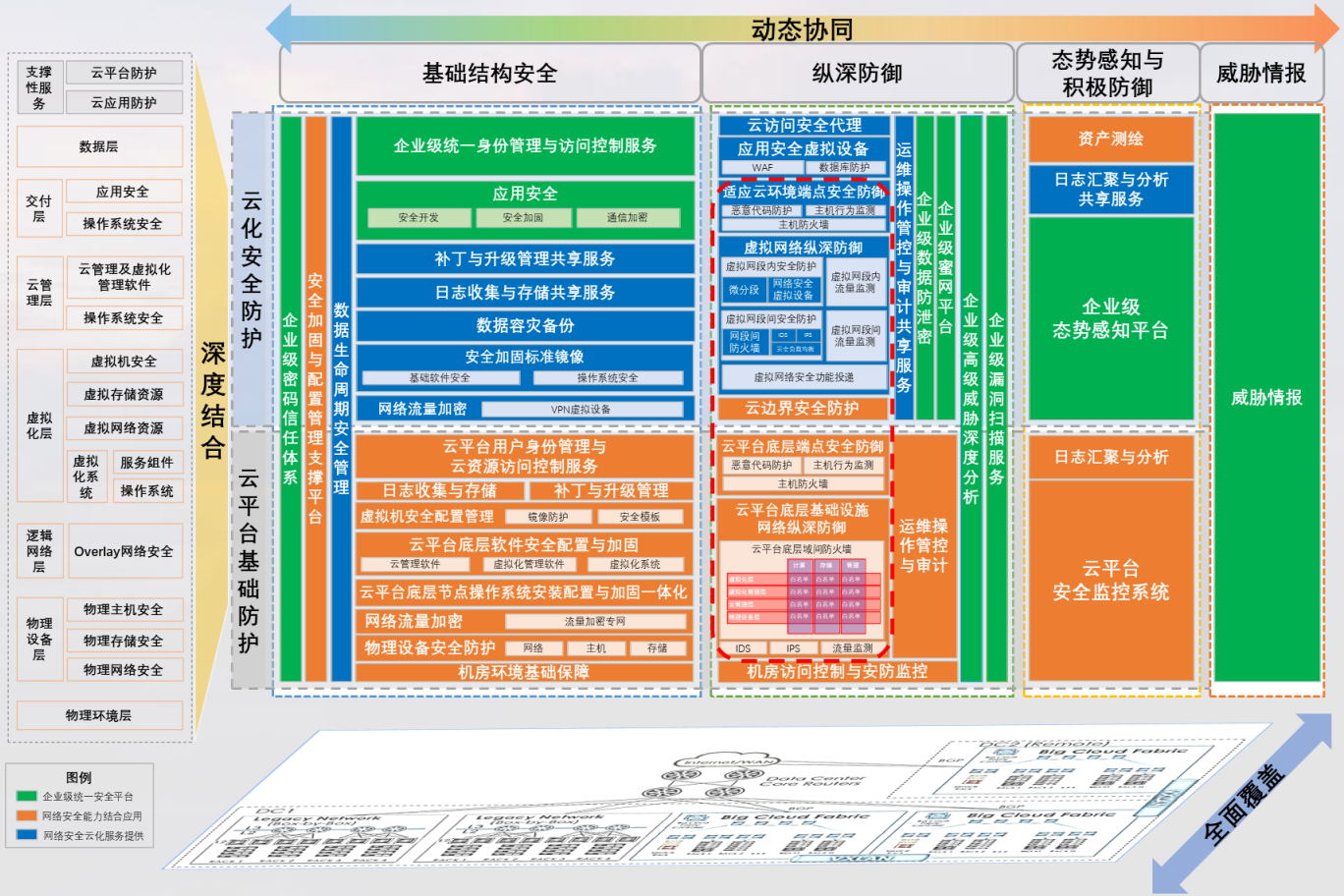
云基础设施与云租户的责任



云基础设施威胁猎杀基础

对云设施建设与运维者，为充分发挥威胁猎杀效果，可逐步建设网络动态综合防御能力。防护与猎杀对象包括：

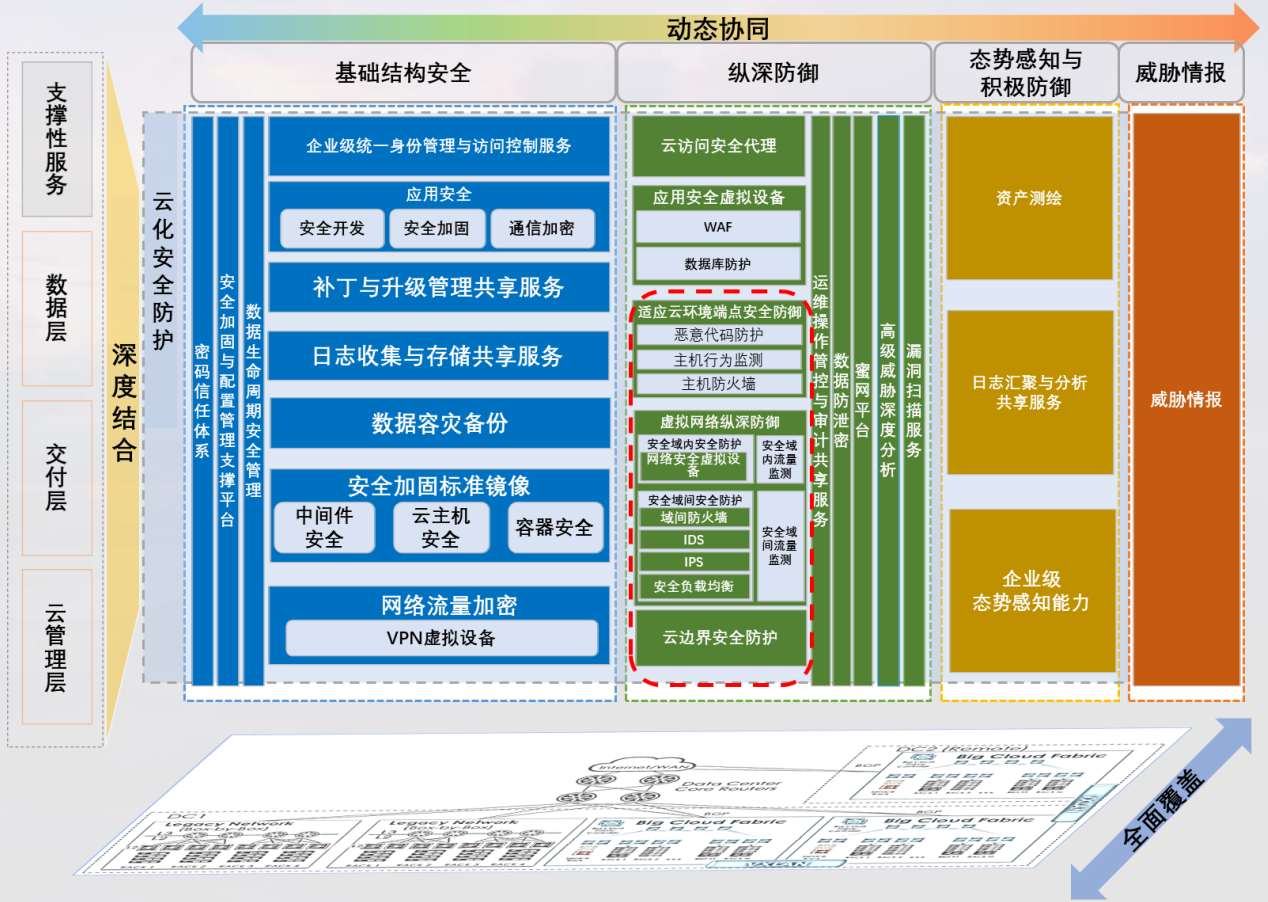
- **云平台基础防护**：构成云的物理环境和物理设备；
- **云化安全防护**：云的逻辑网络、虚拟化、云管理、服务交付和数据等。



云租户云环境威胁猎杀基础

对云租户，为充分发挥威胁猎杀效果，可在云上空间内逐步建设网络动态综合防御能力。防护与猎杀对象包括：

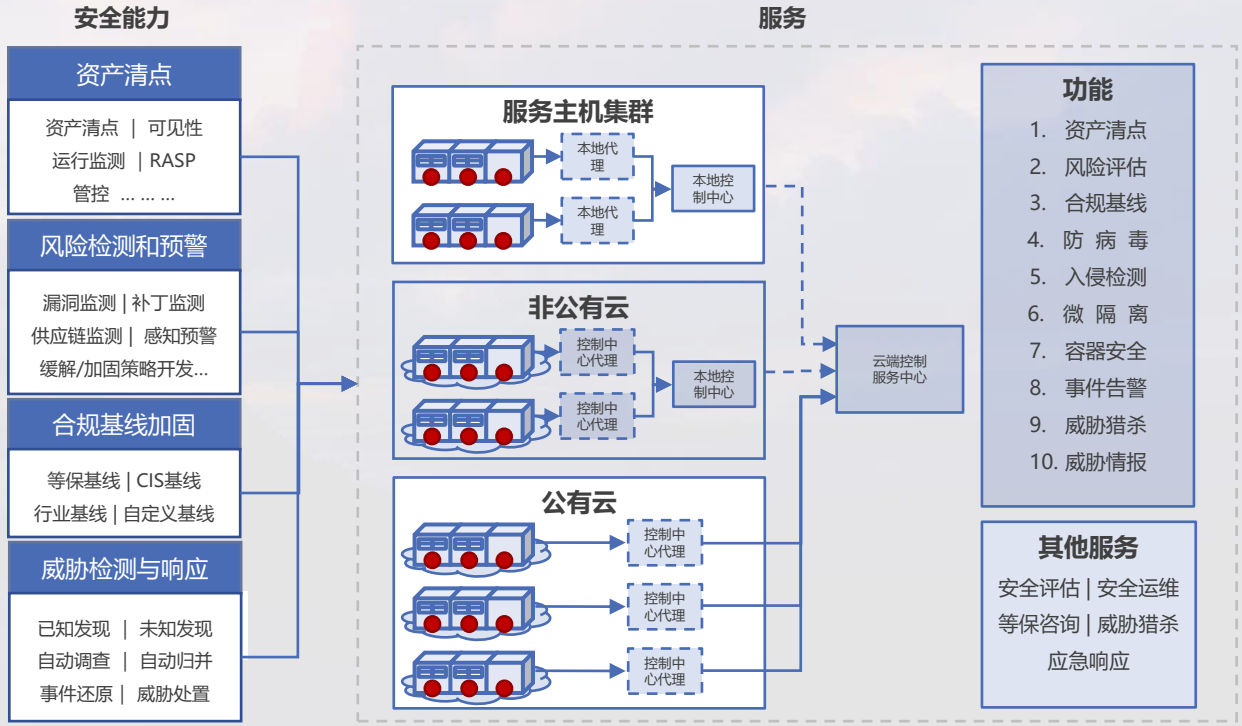
- **虚拟网络：**云上空间的虚拟路由；
- **云主机与容器：**承载业务的主机与容器。
- **应用与数据：**上云的服务与存储的数据



安天智甲云主机安全系统，支撑云环境威胁猎杀

面向多云混合云的 统一云工作负载防护

- 支持物理机、虚拟机、容器等多种工作负载在多云、混合云场景下统一安全防护的需要
- 涵盖资产资产清点、风险评估、合规基线、入侵检测、容器安全、微隔离、容器安全等安全能力
- 支撑威胁猎杀，发现网络攻击线索
- 此外，提供安全评估、安全运维、等保咨询、应急响应等安全服务



系列化云安全产品能力框架图

致敬黄晟老师（大Joe哥）

- 黄晟老师在第一时间建议安天将威胁猎杀作为一个重要的能力建设维度，并特别指出称为“猎杀”比“狩猎”更为精准。
- 黄晟老师深度赋能、持续牵引安天完善动态综合防御模型、威胁猎杀流程体系和成熟度模型。

网络安全资深专家黄晟老师
2021年12月6日在北京不幸逝世， 终年45岁

谨代表安天的工程师们向大Joe哥表达哀思和敬意，他的思想， 他的方法， 他的人格，将永远陪伴着我们，永久融入他热爱并献身的网络安全事业中！

谢谢大家

安天冬训营 wtc.antiy.cn